.$$$ $. .$$$ $.

$$$$ $$. .$$$ $$$ .$$$$$$. .$$$$$$$$$$. $$$$ $$. .$$$$$$$. .$$$$$$.

$ $$ $$$ $ $$ $$$ $ $$$$$$. $$$$$ $$$$$$ $ $$ $$$ $ $$ $$ $ $$$$$$.

$ `$ $$$ $ `$ $$$ $ `$ $$$ $$' $ `$ `$$ $ `$ $$$ $ `$ $ `$ $$$'

$. $ $$$ $. $$$$$$ $. $$$$$$ `$ $. $ :' $. $ $$$ $. $$$$ $. $$$$$.

$::$ . $$$ $::$ $$$ $::$ $$$ $::$ $::$ . $$$ $::$ $::$ $$$$

$;;$ $$$ $$$ $;;$ $$$ $;;$ $$$ $;;$ $;;$ $$$ $$$ $;;$ $;;$ $$$$

$$$$$$ $$$$$ $$$$ $$$ $$$$ $$$ $$$$ $$$$$$ $$$$$ $$$$$$$$$ $$$$$$$$$'

WhatWeb - 下一代网络扫描版本。

Andrew Horton又名urbanadventurer和Brendan Coles开发。

主页: http://www.morningstarsecurity.com/research/whatweb

格式: whatweb [options] <URLs>

目标选择：

<TARGETs> 输入网址, 主机名, IP 地址, 文件名, 或Nmap格式的IP地址范围。 --input-file=FILE, -i 从文件中读取目标。你可以管直接与主机名或URL -i /dev/stdin.

目标修正:

--url-prefix 添加一个前缀到目标网址。

--url-suffix 添加一个后缀到目标网址。

--url-pattern 将目标插入到一个网址中。

e.g. example.com/%insert%/robots.txt

侵略：

侵略级别控制的速度/隐身和之间的权衡可靠性。

--aggression, -a=LEVEL 设置攻击水平。默认值：1。

1. Stealthy 使一个HTTP请求/目标也跟着改变。

3. Aggressive 如果一个1级插件是匹配的，将作出额外的请求。

4. Heavy 让很多的HTTP请求/目标。试图所有插件的网址。

HTTP选项:

--user-agent, -U=AGENT 确定不是WhatWeb /代理。

--header, -H 添加一个HTTP 头. eg "Foo:Bar". 指定一个默认的头将取代他. 指定一个空值, e.g. "用户代理:" 将删除它

--follow-redirect=WHEN 当跟随重定向控制。当可`永远，` HTTP”，`元”，`相同的网站，`同域”或`总是'。默认：总是。

--max-redirects=NUM 重定向的最大数量。默认值：10

认证:

--user, -u=<user:password> HTTP 基本身份验证。

--cookie, -c=COOKIES 使用cookies，例如“名称=值；2 = value2”。

代理:

--proxy <hostname[:port]> 设置代理服务器的主机名和端口。

默认: 8080.

--proxy-user <username:password> 设置代理用户和密码。

插件:

--list-plugins, -l 列出所有插件。

--info-plugins, -I=[SEARCH] 列出所有插件的详细信息。

在逗号分隔的列表中选择搜索关键字。

--search-plugins=STRING 搜索插件的关键字。

--plugins, -p=LIST 选择插件。. 列表是一个逗号分隔的选定插件集。 默认是所有。 每个元素可以是一个目录、文件或插件名称，并且可以选择有一个修改剂， +/-.

例子:+/tmp/moo.rb,+/tmp/foo.rbtitle,md5,+./plugins-disabled/ ./plugins-disabled,-md5 -p + is a shortcut for -p +plugins-disabled.

--grep, -g=STRING 在HTTP响应字符串搜索。一个插件命名grep报告。 --custom-plugin=DEFINITION 定义一个自定义插件名为自定义插件，

例子: ":text=>'powered by abc'"

":version=>/powered[ ]?by ab[0-9]/"

":ghdb=>'intitle:abc \"powered by abc\"'"

":md5=>'8666257030b94d3bdb46e05945f60b42'"

"{:text=>'powered by abc'}"

--dorks=PLUGIN 谷歌为选定的插件列表的呆子。

输出:

--verbose, -v 噜输出包括插件的描述。

使用两次调试

--colour,--color=WHEN 控制颜色是否使用。什么时候可能是“永远”，“永远”，或“汽车”。

--quiet, -q 不显示简短的记录到标准输出。

--no-errors 抑制错误消息。

登录中:

--log-brief=FILE 日志简短，一行输出。

--log-verbose=FILE 日志详细输出。

--log-errors=FILE 记录错误。

--log-xml=FILE 日志XML格式。

--log-json=FILE 日志的JSON格式。

--log-sql=FILE 日志的SQL插入语句。

--log-sql-create=FILE 创建SQL数据库表。

--log-json-verbose=FILE JSON格式的日志冗长。

--log-magictree=FILE magictree XML格式的日志。

--log-object=FILE 日志红宝石对象检查格式。

--log-mongo-database 在MongoDB数据库名称。

--log-mongo-collection 在MongoDB集合名称。

默认值：whatweb。

--log-mongo-host MongoDB的主机名或IP地址。

默认: 0.0.0.0.

--log-mongo-username MongoDB的用户名。默认：无。

--log-mongo-password MongoDB的密码。默认：无。

性能和稳定性

--max-threads, -t 同时线程数。默认值：25。

--open-timeout 秒时间。默认值：15。

--read-timeout 秒时间。默认值：30。

--wait=SECONDS 连接之间的等待秒。

这是有用的，当使用一个单一的线程。

HELP & MISCELLANEOUS:

--short-help 简短使用帮助。

--help, -h 完整的使用帮助。

--debug 提高插件中的错误。

--version 显示版本信息。

使用示例:

\*扫描example.com。

./whatweb example.com

\* 使用详细描述Reddit.com Slashdot.org扫描插件。

./whatweb -v reddit.com slashdot.org

\* 一个积极的扫描连线检测WordPress的确切版本。

./whatweb -a 3 www.wired.com

\* 快速扫描本地网络并抑制错误。

whatweb --no-errors 192.168.0.0/24

\* 扫描HTTPS网站的本地网络。

whatweb --no-errors --url-prefix https:// 192.168.0.0/24

\* 扫描在Alexa排名前1000的跨域政策。

./whatweb -i plugin-development/alexa-top-100.txt \

--url-suffix /crossdomain.xml -p crossdomain\_xml

可选的相关性

--------------------------------------------------------------------------------

使MongoDB测井安装Mongo宝石。